

CompTIA Security+

Learn via: **Classroom/Virtual**

Duration: **5 Days**

Overview

The CompTIA Security+ exam will certify the successful candidate has the knowledge and skills required to install and configure systems to secure applications, networks, and devices; perform threat analysis and respond with appropriate mitigation techniques; participate in risk mitigation activities; and operate with an awareness of applicable policies, laws, and regulations. This course will help delegates prepare for exam SY0-501 - released on October 4, 2017.

Prerequisites

CompTIA Security+ is aimed at IT professionals with job roles such as security architect, security engineer, security consultant/specialist, information assurance technician, security administrator, systems administrator, and network administrator.

Ideally, you should have successfully completed the 'CompTIA Network+ Support Skills' course and have around 24 months' experience of networking support or IT administration. It is not necessary that you pass the Network+ exam before completing Security+ certification, but it is recommended.

Specifically, it is recommended that you have the following skills and knowledge before starting this course:

- Know the function and basic features of the components of a PC.
- Use Windows Server to create and manage files and use basic administrative features (Explorer, Control Panel, Server Manager, and Management Consoles).
- Operate the Linux OS using basic command-line tools.
- Know basic network terminology and functions (such as OSI Model, Topology, Ethernet, Wi-Fi, switches, routers).
- Understand TCP/IP addressing, core protocols, and troubleshooting tools

What You Will Learn

This course will teach you the fundamental principles of installing and configuring cybersecurity controls and participating in incident response and risk mitigation.

Study of the course can also help to build the prerequisites to study more advanced IT security qualifications, including CompTIA Cybersecurity Analyst (CSA)+, CompTIA Advanced Security Practitioner (CASP), and ISC's CISSP (Certified Information Systems Security Professional).

On course completion, you will be able to:

- Identify network attack strategies and defenses.
- Understand the principles of organizational security and the elements of effective security policies.
- Know the technologies and uses of cryptographic standards and products.
- Identify network- and host-based security technologies and practices.
- Describe how wireless and remote access security is enforced.
- Describe the standards and products used to enforce security on web and communications technologies.
- Identify strategies for ensuring business continuity, fault tolerance, and disaster recovery.
- Summarize application and coding vulnerabilities and identify development and deployment methods designed to mitigate them.

Outline

Module 1 / Threats, Attacks, and Vulnerabilities

Indicators of Compromise

- Why is Security Important?
- Security Policy
- Threat Actor Types
- The Kill Chain

- Social Engineering
- Phishing
- Malware Types
- Trojans and Spyware
- Open Source Intelligence

Labs:

- VM Orientation
- Malware Types

Critical Security Controls

- Security Control Types
- Defense in Depth
- Frameworks and Compliance
- Vulnerability Assessments and Pentests
- Security Assessment Techniques
- Pen Testing Concepts
- Vulnerability Scanning Concepts
- Exploit Frameworks

Lab:

- Using Vulnerability Assessment Tools

Security Posture Assessment Tools

- Topology Discovery
- Service Discovery
- Packet Capture & Packet Capture Tools
- Remote Access Trojans
- Honeypots and Honeynets

Labs:

- Using Network Scanning Tools 1
- Using Network Scanning Tools 2
- Using Steganography Tools

Incident Response

- Incident Response Procedures
- Preparation Phase
- Identification Phase
- Containment Phase
- Eradication and Recovery Phases

Module 2 / Identity and Access Management

Cryptography

- Uses of Cryptography
- Cryptographic Terminology and Ciphers
- Cryptographic Products
- Hashing Algorithms
- Symmetric Algorithms
- Asymmetric Algorithms
- Diffie-Hellman and Elliptic Curve
- Transport Encryption
- Cryptographic Attacks

Lab:

- Implementing Public Key Infrastructure

Public Key Infrastructure

- PKI Standards
- Digital Certificates
- Certificate Authorities
- Types of Certificate
- Implementing PKI
- Storing and Distributing Keys
- Key Status and Revocation
- PKI Trust Models
- PGP / GPG

Lab:

- Deploying Certificates and Implementing Key Recovery

Identification and Authentication

- Access Control Systems
- Identification
- Authentication
- LAN Manager / NTL
- Kerberos
- PAP, CHAP, and MS-CHAP
- Password Attacks
- Token-based Authentication
- Biometric Authentication
- Common Access Card

Lab:

- Using Password Cracking Tools

Identity and Access Services

- Authorization
- Directory Services
- RADIUS and TACACS+
- Federation and Trusts
- Federated Identity Protocols

Account Management

- Formal Access Control Models
- Account Types
- Windows Active Directory
- Creating and Managing Accounts
- Account Policy Enforcement
- Credential Management Policies
- Account Restrictions
- Accounting and Auditing

Lab:

- Using Account Management Tools

Module 3 / Architecture and Design (1)

Secure Network Design

- Network Zones and Segments
- Subnetting
- Switching Infrastructure
- Switching Attacks and Hardening
- Endpoint Security
- Network Access Control
- Routing Infrastructure
- Network Address Translation
- Software Defined Networking

Lab:

- Implementing a Secure Network Design

Firewalls and Load Balancers

- Basic Firewalls
- Stateful Firewalls
- Implementing a Firewall or Gateway
- Web Application Firewalls
- Proxies and Gateways
- Denial of Service Attacks
- Load Balancers

Lab:

- Implementing a Firewall

IDS and SIEM

- Intrusion Detection Systems
- Configuring IDS
- Log Review and SIEM
- Data Loss Prevention
- Malware and Intrusion Response

Lab:

- Using an Intrusion Detection System

Secure Wireless Access

- Wireless LANs
- WEP and WPA
- Wi-Fi Authentication
- Extensible Authentication Protocol
- Additional Wi-Fi Security Settings
- Wi-Fi Site Security
- Personal Area Networks

>

Physical Security Controls

- Site Layout and Access
- Gateways and Locks
- Alarm Systems
- Surveillance
- Hardware Security
- Environmental Controls

Module 4 / Architecture and Design (2)

Secure Protocols and Services

- DHCP Security
- DNS Security
- Network Management Protocols
- HTTP and Web Servers
- SSL / TLS and HTTPS
- Web Security Gateways
- Email Services
- S/MIME
- File Transfer
- Voice and Video Services (VoIP and VTC)

Labs:

- Implementing Secure Network Addressing Services
- Configuring a Secure Email Service

Secure Remote Access

- Remote Access Architecture
- Virtual Private Networks
- IPSec
- Remote Access Servers
- Remote Administration Tools
- Hardening Remote Access Infrastructure

Lab:

- Implementing a Virtual Private Network

Secure Systems Design

- Trusted Computing
- Hardware / Firmware Security
- Peripheral Device Security
- Secure Configurations
- OS Hardening
- Patch Management
- Embedded Systems
- Security for Embedded Systems

Secure Mobile Device Services

- Mobile Device Deployments
- Mobile Connection Methods
- Mobile Access Control Systems
- Enforcement and Monitoring

Secure Virtualization and Cloud Services

- Virtualization Technologies
- Virtualization Security Best Practices
- Cloud Computing
- Cloud Security Best Practices

Module 5 / Risk Management

Forensics

- Forensic Procedures
- Collecting Evidence
- Capturing System Images
- Handling and Analyzing Evidence

Lab:

- Using Forensic Tools

Disaster Recovery and Resiliency

- Continuity of Operations Plans
- Disaster Recovery Planning
- Resiliency Strategies
- Recovery Sites
- Backup Plans and Policies
- Resiliency and Automation Strategies

Risk Management

- Business Impact Analysis
- Identification of Critical Systems
- Risk Assessment
- Risk Mitigation

Secure Application Development

- Application Vulnerabilities
- Application Exploits
- Web Browser Exploits
- Secure Application Design
- Secure Coding Concepts
- Auditing Applications
- Secure DevOps

Lab:

- Identifying a Man-in-the-Browser Attack

Organizational Security

- Corporate Security Policy
- Personnel Management Policies
- Interoperability Agreements
- Data Roles
- Data Sensitivity Labeling and Handling
- Data Wiping and Disposal
- Privacy and Employee Conduct Policies
- Security Policy Training